

### **Remarks**

Applicant respectfully requests that this Amendment After Final Action be admitted under 37 C.F.R. § 1.116.

Applicant submits that this Amendment presents claims in better form for consideration on appeal. Furthermore, applicant believes that consideration of this Amendment could lead to favorable action that would remove one or more issues for appeal.

Claim 1 has been amended. No claims have been canceled. Therefore, claims 1-15 are now presented for examination.

Claims 1, 2, 10, 13 and 14 stand rejected under 35 U.S.C. §103(a) as being anticipated by Cromer et al. (U.S. Patent No. 6,684,326), in view of Cooper et al. (U.S. Patent No. 5,961,588). In addition, claim 7 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Cromer in view of Cooper, with Office Notice taken.

Applicant submits that the present claims are patentable over Cromer in view of Cooper.

Cromer discloses a method and system for performing an authenticated boot of a computer system in a networked computing environment. The system includes integrates boot manager services into a power on self test (POST) routine of a client system. The client system provides a digital signature for a selected operating system when the POST routine transfers control to a basic input/output system (BIOS) routine. Booting is authorized with the operating system through authentication by a server system of the digital signature. See Cromer at col. 1, ll. 47-57.

Cooper discloses a client station and method for controlling a telecommunications system. The telecommunications system includes a central station and a server station.

The server station is arranged to maintain an object model thereon representing the central station, and is connectable to the central station to send control signals to the central station in accordance with the object model. The client station comprises a communications manager for establishing first and second interfaces with the server station to enable communication between the client station and the server station, thereby to manage the object model maintained on the server. The client station has a memory for storing a portion of the object model, and a processor for processing commands received by the client station via the first interface from a queue maintained on the server station. Further, there is provided a retrieval means, responsive to a command requiring an operation to be performed on an object not currently in the portion of the object model stored in the memory, for retrieving from the server station via the second interface said object for inclusion in the portion of the object model stored in the memory, during which time no further commands are processed by the processor. See Cooper at Abstract.

Claim 1 of the present application recites a client computer to access an authentication stack during a power on self-test (POST) that enables authentication of the remote server for authorization to boot the client computer. Applicant submits that neither Cromer nor Cooper disclose or suggest a client computer authenticating a remote server to enable the server to boot the client computer. Cromer discloses authenticating an operating system at the computer system that is to boot a the computer system. However, there is no disclosure in Cromer of the server booting the client system.

Since both Cromer and Cooper fail to disclose or suggest a client computer authenticating a remote server to enable the server to boot the client computer, any

combination of Cromer and Cooper would also fail to disclose or suggest such a feature.

Therefore claim 1 and dependent claims 2-15 are patentable over Cromer.

Claims 3, 4, 8, and 9 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Cromer et al., in view of Cooper et al., as established above, and further in view of Angelo (U.S. Patent No. 6,953,422). Applicant submits that the present claims are patentable over Cromer and Cooper even in view of Angelo.

Angelo discloses a computer system incorporating a two-piece authentication procedure for securely providing user authentication over a network. A user password is entered during a secure power-up procedure. The user password is encrypted by an external token or smart card that stores an encryption algorithm furnished with an encryption key that is unique or of limited production. A network password is thereby created. The network password is maintained in a secure memory space such as System Management Mode (SMM) memory. The network password is then encrypted and communicated over the network. The network password may be encrypted using the server's public key or another key that is known to the server. Optional node identification information is appended to the network password prior to communication over the network. Once received by the server, the encrypted network password is decrypted using the server's private key. A user verification process is then performed on the network password to determine which, if any, access privileges have been accorded the network user. See Angelo at Abstract.

However, Angelo does not disclose or suggest a client computer authenticating a remote server to enable the server to boot the client computer. As discussed above, Cromer and Cooper also fail to disclose or suggest a client computer authenticating a

remote server to enable the server to boot the client computer. Thus, any combination of Cromer and Angelo would not disclose or suggest a client computer authenticating a remote server to enable the server to boot the client computer. As a result, the present claims are patentable over Cromer and Cooper in view of Angelo.

Claims 5, 6, 11 and 12 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Cromer, in view of Cooper, in view of Angelo, as established above, and further in view of Novoa et al. (U.S. Patent No. 6,223,284). Applicant submits that the present claims are patentable over Cromer, Cooper and Angelo even in view of Novoa.

Novoa discloses a remote flash ROM and security package formed and delivered to a system ROM of a target computer system for remote flashing of the ROM and remote configuration of security settings for the computer system. See Novoa at Abstract. Nevertheless, Novoa does not disclose or suggest a client computer authenticating a remote server to enable the server to boot the client computer. As discussed above, neither Cromer, Cooper nor Angelo disclose or suggest a client computer authenticating a remote server to enable the server to boot the client computer. Thus, any combination of Cromer, Cooper, Angelo and Novoa would not disclose or suggest such a feature. As a result, the present claims are patentable over the combination of Cromer, Cooper, Angelo and Novoa.

Claim 15 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Cromer., in view of Cooper., further in view of Angelo, as established above, and further in view of Bisbee (U.S. Pub. No. 2001/002485). Applicant submits that the present claims are patentable over Cromer, Cooper and Angelo even in view of Bisbee.

Bisbee discloses a method of handling stored e-original objects that have been created by signing information objects by respective Transfer Agents, submitting signed information objects to a TCU, validating the submitted signed information objects by at least testing the integrity of the contents of each signed information object and the validity of the signature of the respective Transfer Agent, and applying to each validated information object a date-time stamp and a digital signature and authentication certificate of the TCU. See Bisbee at Abstract.

Nonetheless, Bisbee does not disclose or suggest a client computer authenticating a remote server to enable the server to boot the client computer. As discussed above, both Cromer, Cooper and Angelo fail disclose or suggest such a feature. Thus, any combination of Cromer, Cooper Angelo and Bisbee would not disclose or suggest the feature. As a result, the present claims are patentable over the combination of Cromer, Cooper, Angelo and Bisbee.

Applicant respectfully submits that the rejections have been overcome, and that the claims are in condition for allowance. Accordingly, applicant respectfully requests the rejections be withdrawn and the claims be allowed.

The Examiner is requested to call the undersigned at (303) 740-1980 if there remains any issue with allowance of the case.

Please charge any shortage to our Deposit Account No. 02-2666.

Respectfully submitted,  
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Date: December 2, 2005

---

Mark L. Watson  
Reg. No. 46,322

12400 Wilshire Boulevard  
7<sup>th</sup> Floor  
Los Angeles, California 90025-1026  
(303) 740-1980